10 points for each question

1. The CFB mode discussed in class can be generalized into a k-bit CFB mode by only taking the first k bits of the output of a block encryption and XOR with k bits of the plaintext. If a bit error occurs in the transmission of a ciphertext character in 8-bit CFB mode with DES, how far does the error propagate? That is, how many blocks does the error affect (including itself)?

2. For CBC, OFB, and CTR operation modes, what's the main goal of using initialization vectors? Does an initialization vector need to be a secret value?

3. What are semi-weak keys for DES? Assume that the first permutation output of an original key to DES is semi-weak. Describe a possible attack against DES encryption? Does this attack significantly reduce the security of DES? Please justify your answer.

4. Show that DES encryption and decryption are identical except for the order of the 48-bit keys. (Hint: running a round backwards is the same as running it forwards but with the halves swapped, and DES has a swap after round 16 when run forwards).

5. John Smith works at a company that makes network storage systems. He is given a task to design a method to allow encryption of files stored in the system. In other words, all files are stored in an encrypted form. If a host using the storage system requests a block of a file, the system should retrieve the block, decrypt it and return the plaintext to the host. Similarly, if a host writes a block to the storage system, the system should retrieve the right keying material, encrypt the block, and only save the ciphertext on disk. Consider the block cipher modes. Which one should be used? Why?

6. What are the desired properties of hash functions?

7. Alice needs to send *n* packets to Bob. Alice and Bob wish to use *n* different random one-time pads to encrypt the *n* packets. The encryption is simply bit-wise XORing a packet and an one-time pad. Assume each packet is of 128 bits. Describe how Alice and Bob can generate *n* different one-time pads by using a shared secret key *S* and a cryptographic hash function *h*.

8. Alice developed a message authentication code (MAC) based on DES. Her algorithm works as follows: For a given input message M, represent M as M = (X1 || X2 || ... || Xm), where Xi is a 64-bit block and || represents concatenation. Compute Delta(M) = X1 ^ X2 ^ ... ^ Xm, where ^ represents bit-wise XOR. Then the MAC for M is computed as C_K(M) = E_K(Delta(M)), where E is DES encryption algorithm and K is the secret key. Unfortunately, this scheme is vulnerable. Describe an attack against it.

9. Textbook 4.5.3: Let’s assume you do DES double encryption by encrypting with K1 and doing DES in decrypt mode with K2. Does the same attack work as with double encryption with K1 and K2? If not, how could it be made to work.

10. Textbook 4.5.4: What is a practical method for finding a triple of keys that maps a given plaintext to a given ciphertext using EDE.